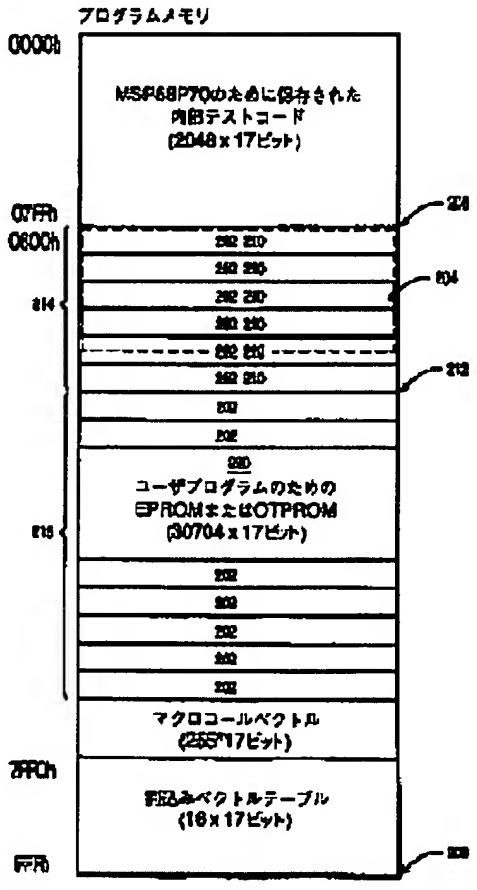
SECURITY GUARANTEE METHOD FOR PROGRAM DATA INSIDE MEMORY WRITABLE ONLY ONCE

Publication number: JP2000076133
Publication date: 2000-03-14
Inventor: HENDERSON ALVA; FRANCESCO CABARIELE
Applicant: TEXAS INSTRUMENTS INC
Classification:
- international: ***G06F12/14; G11C16/02;*** **G06F12/14; G11C16/02;** (IPC1-7): G06F12/14; G11C16/02
- european:
Application number: JP19990158533 19990604
Priority number(s): US19980087957P 19980604; US19980089572P 19980617; US19980090668P 19980625

Report a data error here

Abstract of **JP2000076133**

PROBLEM TO BE SOLVED: To provide a method for protecting data and a program code stored inside an EPROM array from the act of piracy. SOLUTION: After the completion of first programming starting from the first memory address of a nonvolatile memory array 220, a second address 208 from the last functioning as a protective register is set and made to correspond to the number of a protective block 210. For that, a section boundary 212 is set and the array is divided. When the bit 7 (block protection) of the protective register is enabled (set to zero), the contents of a primary security section 214 made non-readable and non-writable. The protective register is written by both of the number of the protective block and the inversion. It prevents the unauthorized change of the protective register and the movement of the section boundary because writing only 0 in the EPROM.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－76133
（P2000－76133A）
(43)公開日　平成12年３月14日(2000.3.14)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｄ	
Ｇ１１Ｃ　16/02		Ｇ１１Ｃ　17/00	６１１Ｚ	

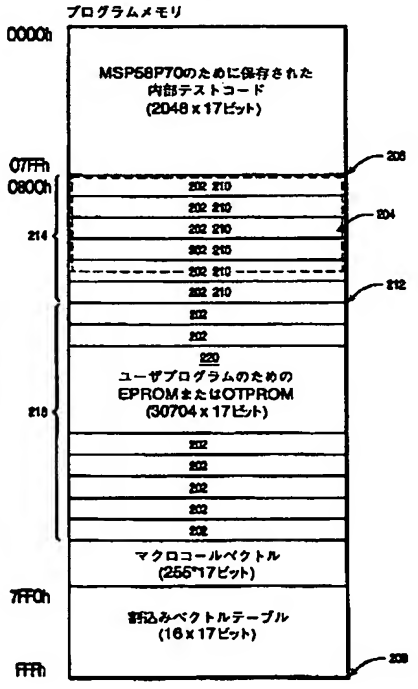
審査請求　未請求　請求項の数１　ＯＬ　（全 ９ 頁）

(21)出願番号　特願平11－158533
(22)出願日　平成11年６月４日(1999.6.4)
(31)優先権主張番号　０８７９５７
(32)優先日　平成10年６月４日(1998.6.4)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　０８９５７２
(32)優先日　平成10年６月17日(1998.6.17)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　０９０６６８
(32)優先日　平成10年６月25日(1998.6.25)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　590000879
テキサス　インスツルメンツ　インコーポレイテツド
アメリカ合衆国テキサス州ダラス，ノース　セントラルエクスプレスウエイ　13500
(72)発明者　アルバ　ヘンダーソン
アメリカ合衆国　テキサス，シャーマン，プレストン　クラブ　ドライブ　228
(72)発明者　フランセスコ　カバリエレ
アメリカ合衆国　テキサス，プラノ，オアリイ　コート　7704
(74)代理人　100066692
弁理士　浅村　皓　（外３名）

(54)【発明の名称】　一度だけ書込み可能なメモリ内のプログラムデータのセキュリティ保証方法

(57)【要約】
【課題】　ＥＰＲＯＭアレイ内に記憶されたデータとプログラムコードを海賊行為から保護する方法を得る。
【解決手段】　非揮発性メモリアレイ２２０の第１のメモリアドレスから始まる最初のプログラミングの完了後に、保護レジスタとして働く最後から２番目のアドレス２０８がセットされて、保護ブロック２１０の番号と対応する。これは、セクション境界２１２をセットして、アレイを分割する。１次セキュリティ・セクション２１４の内容は、保護レジスタのビット７（ブロックプロテクト）がイネーブル（ゼロにセット）されると、読取り不可で書込み不可にされる。保護レジスタは、保護ブロックの番号およびその反転の両方で書き込まれる。これは、ＥＰＲＯＭが０しか書けないことにより、保護レジスタを不正に変更してセクション境界を移動することを防止する。



【特許請求の範囲】
【請求項１】　プログラムメモリと、
複数のプログラムの少なくとも２つのクラスの間の前記プログラムメモリの部分のためのアクセス特権を指示するセキュリティ・レジスタと、
前記プログラムメモリの第１の部分から複数のプログラムの第１のクラスを実行し、前記プログラムメモリの少なくとも１つの他の部分から複数のプログラムの少なくとも１つの他のクラスを実行するために接続されたプログラマブル・プロセッサとを含み、
前記プログラムブル・プロセッサ論理は、前記セキュリティ論理の制御の下においてのみ、また、前記セキュリティ論理がデータ・ポインタとアドレス・ポインタとの間の両立可能な所有権を指示するときにのみ、前記メモリにアクセスできる、
集積回路。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンピュータ・マイクロプロセッサに関し、特に、１度だけ書込み可能な（ＯＴＰ）内部メモリを特徴とするマイクロプロセッサに関する。
【０００２】
【従来の技術】コンピュータおよびマイクロコントローラ内のパーマネント・オペレーティング・コード
コンピュータまたはマイクロプロセッサは、典型的には、電源を切っても符号（コード）が保持されるように非揮発性メモリ（たとえば、ＲＯＭ、ＥＰＲＯＭ、フラッシュメモリ）内に記憶されたそのオペレーティング・コードの重要部分を有する。しばしば、この符号の全てまたは一部は、中央処理装置（ＣＰＵ）自体として同一チップ上に常駐するメモリ（内部メモリ）内に記憶される。これにより、ＣＰＵおよびその基本オペレーティング・コードを単一ユニットとして実装（パッケージ）可能にしている。単一チップ内での諸機能のこの集積は、プロセッサを使用するアセンブリの設計を単純化するのに役立つ。この集積はまた、部品数（part count）を減少させ、信頼性を向上するのに役立つ。
【０００３】ＯＴＰメモリに記憶されたパーマネント・オペレーティング・コード
多くのマイクロプロセッサ、特にマイクロコントローラとして知られるクラスのマイクロプロセッサは、ＵＶ消去可能ＥＰＲＯＭ，ＥＥＰＲＯＭ，１度だけプログラム可能な（ＯＴＰ）メモリまたはフラッシュメモリのような電気的にプログラム可能な読取り専用メモリ（ＥＰＲＯＭ）のある形で、それらの内部オペレーティング・コードを記憶する。この設計により、ＩＣの製造後にオペレーティング・コードをプログラムすることが可能になり、ＲＯＭに基づく設計よりも遥かに高度な柔軟性をもたらす。このアーキテクチャーによれば、製造者は、製造後にオペレーティング・コードを改定し改良したり、オペレーティング・コードを特別の注文により変更して複数の顧客の特別なニーズに応えることができる。代りに、製造者は、ＥＰＲＯＭバンクを空白のままにしたり部分的にプログラムして、顧客がその固有のコードをインストールできるようにし得る。この設計により、製造者は一層大量のチップを１度に設定できるようになり、特殊な手持ち在庫の必要を減少させ、迅速なプロトタイピングを容易にする。
【０００４】オンチップ・ソフトウェアのセキュリティ
多くの場合、チップをプログラムする人（製造者または他のパーティ）は、機密保持のために彼が好ましいと思うソフトウェア・コードでチップをプログラムする。そうした場合、先のプログラマーは、後のプログラマーおよびユーザを制約して、チップのメモリバンクからの読取りおよびコピーができないようにするとともに、その中に記憶されたコードの実行のためのアクセスができるようにしておくことを望むであろう。製造者は、チップの内部メモリの一部分をプログラムするとともに、内部メモリの残部を顧客がプログラムするために開放することを望むかもしれない。そうした場合、プログラマーの一方または両方は、他のプログラマーおよび第三者からこのコードを保護しようと望むかもしれない。
【０００５】許可されてないコピーに対するメモリの保護は、複雑で困難な課題である。保護つきメモリは、通常、何かに使用するためにはプロセッサが読めなければならないコードおよびコード関連データを含む。一層問題なことに、ＣＰＵの制御を後のプログラマーおよびユーザへ明け渡さなければならず、彼らの多くが先のプログラマーに対して相反する利害を有するであろう。設計においてそれらの道を閉ざすために、あらゆる保護方式は迂回の可能な道を予想しなければならない。
【０００６】現在のメモリセキュリティ方式は、内部メモリバンクを一単位としてロックする。最初のプログラマーがメモリの一部分をプログラムするとともに他の部分を顧客のために残したいと望む場合は、読取りプロテクトを機能抑止のままにして、この最初のプログラマーのソフトウェアが保護されないままにしておかなければならない。装置に精通した人々にとっては、セキュリティ保護を迂回する道が一つ以上あるのが普通であり、これが主としてたまにしか使用しない人に対してそうしたセキュリティを有効なものにしている。
【０００７】アレイの一つだけのプログラマー定義可能セクションの保護が可能であり、このアレイの残りの部分のプログラミングが可能なソフトウェア・セキュリティ方式は、現在のところ存在しない。
【０００８】
【発明が解決しようとする課題】ブロック区分されたセキュリティ・メモリ
本出願は、各パーティのコードについて完全なセキュリ

ティ保護を有する２つ以上のパーティにより装置をプログラムできる方式を記述する。本発明は、製造者が基本ルーチンを装置へプログラムすることを可能にし、また、開発者が各プログラマー・コードについて完全なセキュリティ保護を有する特定アプリケーション用の装置を更にプログラムすることを可能にする。一つの代りの実施の形態において、エンドユーザまたは他の後続のプログラマーが、特定設置に固有な保護つきコードを追加できる。本出願において開示されるセキュリティ回路および制御は、他のプログラマーとともにあらゆる第三者からの海賊行為に対して強力な保護を各プログラマーに提供する。

【０００９】

【課題を解決するための手段】好ましい実施の形態では、第１のプログラマーが定義可能な２つ以上のセクションに非揮発性メモリアレイを分割することにより、セキュリティ保護が達成される。一つのセクションがプログラムされロックされると、どのプログラマーもユーザもいずれの保護つきセクションへも読取りまたは書込みのアクセスができず、確立されたセクション境界も変更できない。命令アドレスと同じメモリセクション内のメモリアドレスをＣＰＵが参照する場合には、読取り命令はＣＰＵによってのみ実行される。異なったセクション内のアドレスを読むことのＣＰＵへの命令は、単純に無視される。

【００１０】本出願は、１次セキュリティ方式の迂回を防止するために設計された多数の他の機能を開示する。プロセッサは、コードセクション境界自体の値を保護する機構を採用し、また、保全されたコードを保護するために種々の新規な方式が採用される。ＣＰＵは、その内蔵テストモードの一つにある。これらの機構を通じて、競争者や顧客による海賊行為から自分のコードが保全されるという高度の確信をもって、開発者はこのＣＰＵ上に彼のコードをインストールできる。

【００１１】開示された方法および構造の一つの利点は、メモリの一つのセクションのプログラミングおよび読取りを可能にするとともに、読取りまたはプログラムの操作から安全なセクションを完全に保護することである。

【００１２】

【発明の実施の形態】開示される発明は添付図面を参照して説明されるが、これらは本発明の重要な実施の形態を示し、また、本明細書に参考として組み込まれたものを示す。本発明の多数の技術革新的な教示について、現在好ましい実施の形態を特別に参照しながら説明する。しかしながら、このクラスの実施の形態は本明細書の技術革新的な教示の多くの有利な利用のほんの少しの例を提供するだけであることを理解すべきである。一般に、本出願の明細書になされる供述は、必ずしも、本発明の種々のクレームされた発明のいずれかを限定するものではない。その上、いくつかの供述は、本発明のいくつかの機能に適用できるが、他の機能には適用できない。

【００１３】メモリセクション保護の動作

図２を参照すると、非揮発性メモリ２２０は、その設計により、２つ以上のブロック２０２に分割されている。最初のプログラマーによりプログラムされたコード２０４は、一つ以上のブロック２０２を占め、第１のメモリアドレス２０６で始まる。初期プログラミングが完了した後に、アレイ２００（保護レジスタ）の最後から２番目のアドレス２０８が保護ブロック２１０の数に対応してセットされる。これにより、セクション境界２１２をセットし、このアレイを１次セキュリティ・セクション２１４と２次セキュリティ・セクション２１６とに分割する。１次セキュリティ・セクション２１４の内容は、保護レジスタ（ブロック保護）のビット７が有効化される（ゼロにセットされる）と、読出し不能で書込み不能にされる。

【００１４】保護値のセキュリティ

好ましい実施の形態では、保護レジスタのビット９～１５は、保護されるブロックの番号を反映する値で書き込まれるが、ビット０～６はその値の１の補数（論理反転）で書き込まれる。たとえば、“１０１１　１００１”の１の補数は、“０１００　０１１０”である。この反転値検証方式は、第２のプログラマーの制御の下にあるメモリの部分内に保護レジスタが配置されているという事実により必要とされ、ブロック保護が有効化された後でも変更され得る。本発明で採用されるこの反転値検証方式は、ＥＰＲＯＭビットのデフォルト値が１であり、プログラミング中に１ビットをクリアできるが１に戻せない（すなわち、ゼロのみがＥＰＲＯＭセルに書き込まれ得る）という事実の利点を有する。ＥＰＲＯＭ内の８ビット語は製造者では“１１１１　１１１１”を登録する。たとえば、第１のプログラマーは、それを“１１１１　００００”にプログラムする。それから、この語は、“１０１０　００００”にプログラムできるが、“１１１１　０１０１”にはプログラムできない。

【００１５】保護値自体だけがインデックスとして使用される場合には、単に保護コードをクリアするだけで後続のプログラマーがセキュリティ方式を完全に打ち負かすことができる。これにより、セクション境界をゼロにロールバックして、メモリアレー全体を彼の制御下に置くことができる。その後、このプログラマーは、第１のプログラマーのコードを含むアレイの内容全体をプロセッサの出力ポートの一つにコピーすることができる。

【００１６】一方、反転値のみが使用される場合には、保護されてない領域に「トロイの木馬」プログラムを書き込んだのちに保護値をクリアすることによって、後続のプログラマーはこのセキュリティ方式を打ち負かすことができる。これにより、セクション境界をメモリの終点へ移動する。トロイの木馬プログラムは、元のコード

と同じセクション境界の背後にある。その後、セキュリティ回路は、トロイの木馬がメモリアレイ全体にアクセスすることを許容する。その後、このプログラムは、プロセッサの出力ポートにアレイ全体をコピーする。好ましい実施の形態で利用される方式によれば、第２のプログラマーは、ビット０～６を直して、ビット９～１５の修正値の補数にすることができない。たとえば、元の保護値が“１０１　００１１”であれば、正しい補数は“０１０　１１００”である。第２のプログラマーはこの保護値を“０００　００００”に変えることができる。しかしながら、ＥＰＲＯＭに書き込むことができないので、この補数を“０１０１１００”から“１１１１１１１”へ変更できない。セキュリティ回路は、この不一致を検出して、アレイへの全ての読取りおよび書込みを機能抑止するであろう。

【００１７】メモリ保護回路

いったん保護値がプログラムされ、ブロック保護が使用可能にされると、調べられる命令アドレスおよびアドレスが同一セクション内（すなわち、セクション境界の同一側）にない限り、ＣＰＵはどんなテーブル・ルックアップ命令も実行しない。

【００１８】このセキュリティチェックを行うために、この装置は、プログラムカウンタ（現に実行される命令のアドレス）およびデータ・ポインタ（現に作用されるメモリアドレス）の両方を保護値と比較する。両方が、保護値よりも高いか低くなければならない。ブロック保護が使用許可になった後で保護値（セクション境界）の同一側にこの２つのアドレスが存在しないと、テーブル・ルックアップまたは書込み命令は何も実行されない。

【００１９】このセキュリティチェックを遂行する回路を図１に示す。保護レジスタ１８４のビット９～１５の内容は、プログラムカウンタ・コンパレータ１０２およびデータポインタ・コンパレータ１０４の両方の入力Ｂにロードされる。プロセッサプログラム・カウンタ１０８の最上位７ビット（すなわち、最寄のブロック全体への命令アドレス）のブロック１０６が、プログラムカウンタ・コンパレータ１０６の入力Ａにロードされる。プロセッサ・データポインタ１１２の最上位７ビット（すなわち、最寄のブロック全体への命令オペランドのメモリアドレス）のブロック１１０が、データポインタ・コンパレータ１０４の入力Ｂにロードされる。入力Ａの値が入力Ｂの値よりも大きいか等しければ、各コンパレータ出力が論理「真」を出力する。

【００２０】２つのコンパレータ１０２，１０４の出力１１４，１１６は排他的論理和（ＸＯＲ）ゲート１１８に送られる。コンパレータ１０２，１０４の出力１１４，１１６が異なれば（すなわち、アドレスが異なったセクションにあれば）、ＸＯＲゲート１１６の出力１２０は真であるが、さもなければ、偽である。ＸＯＲゲート１１８の出力１２０は、ＡＮＤゲート１２４の１つの入力１２２に送られる。ＡＮＤゲート１２４の他の入力１２６には、ブロック保護ビット７が供給される。ブロック保護が使用可能にされ、かつ、命令およびオペランド（データ）のアドレスが同一セクション内になければ、ＡＮＤゲート１２４の出力１２８は真である。この出力１２８は、以下の仕方で回路により使用される。

【００２１】ブロック保護回路の第２の部分は、保護レジスタ内に記憶された保護値で調整することから保護するように設計されている。この回路は、保護値の１の補数（論理反転）であることを期待されるチェック値と保護値を比較する。ブロック保護が使用可能にされるときにチェック値が保護値の反転でなければ、プロセッサは全てのルックアップ命令を完全に機能抑止する。

【００２２】この比較を行うための回路も図１に示されている。保護レジスタのビット０～６は、７ビット排他的論理和（ＸＯＲ）ゲート１５２の一つの入力１５０に送られる。保護レジスタのビット９～１５は、同じＸＯＲゲート１５２の他の入力１５４に送られる。ビット０～６の各々がビット９～１５の対応するビットの論理反転であれば（すなわち、調整（不正な変更）がなければ）、このゲート１５２の出力１５６は偽になる。不一致があれば（すなわち、保護値またはチェック値が不正に変更されていれば）、出力１５６は真である。ＸＯＲゲート１５２の出力１５６はＡＮＤゲート１５８の一つの側に送られる。ＡＮＤゲート１５８への他の入力１６０には、保護レジスタ１００のブロック保護使用可能ビット７が供給される。反転チェック値に不一致があり、かつ、ブロック保護が使用可能にされていれば、ＡＮＤゲート１５８からの出力１６２は真である。

【００２３】その後、セクタ比較回路からの出力１２８と保護値セキュリティ回路からの出力１６２とは、ＯＲゲート１６４に送られる。このゲート１６４からの出力１６６は、他のプロセッサ論理１８０に送られ、それが真であるときに全てのルックアップ（すなわち、読取り）命令を機能抑止する。したがって、ブロック保護が使用可能にされているときにセクタ境界が突破されるか保護値が不正に変更されれば、プロセッサは全てのルックアップ命令を機能抑止する。更に、この出力１６６は、第２のＯＲゲート１６８にも送られる。他の入力１７０は、保護レジスタからのグローバル保護ビット８の状態を反映する。このＯＲゲート１６８からの出力１７２は、他のプロセッサ論理１８２に送られ、それが真であるときにＥＰＲＯＭアレイへのあらゆる読取りおよび書込み動作を完全に機能抑止する。

【００２４】テストモード中のメモリセキュリティ保護

プロセッサのテストモード特にエミュレーションおよびトレース・テストモードの使用を通じて保護メモリへのアクセスをプログラマーが得ることを防止するために、保護の第２の層が装備される。エミュレーション・モードでは、プロセッサは命令を実行しデータレジスタを読

み取るが、これは内部メモリからのように外部メモリからメモリ保護値を読み取ることを含む。トレース・モード（トレース１およびトレース２）では、プロセッサは、ユーザによって制御されたタイミングおよびブレークポイントに従う内部命令を実行する。

【００２５】エミュレーション・モードとトレース・モードとの間を自由に移行できることにより、プログラマーがかなり容易にセキュリティ回路を迂回できる。プログラマーは、異なった保護値（たとえば、“００００００”）を外部メモリに記憶させて、エミュレーション・モードを使用して新しい保護値の使用をプロセッサに強制できる。その後、彼は、トレース・モードに移行して、内部メモリ内の既に保護されたプログラムを１度に１命令ずつウォーク・スルーすることができる。テスト作業モードがスイッチされる前に装置を初期化するようにプログラマーに強制することにより、このプロセッサは上記策略をブロックできる。初期化に際して、プロセッサは内部ＥＰＲＯＭの最期から２番目のメモリ位置から直接に保護値を読み取る。これにより、贋の保護値の使用により引き起こされるセキュリティ回路のあらゆる混乱に対して安全にできる。

【００２６】ＭＳＰ５８７０プロセッサ・アーキテクチャー

セキュリティ方式は、本来は、消費者電子製品用に設計された低コスト混合信号プロセッサへ組み込まれていた。混合信号プロセッサのブロック図を図３Ａおよび図３Ｂに示す。

【００２７】好ましい実施の形態によるプロセッサ１０は、プログラムデータメモリブロック１１およびデータメモリブロック１２を含むいくつかの主要サブブロックを含む。主要サブブロックは、計算ユニット（ＣＵ）１３と、データメモリアドレスユニット（ＤＭＡＵ）１４と、プログラムカウンタ（ＰＣＵ）１５と、命令デコーダ１６とを含む。その他の機能は、反復または連鎖カウンタレジスタ１７とステータスレジスタ１８と２つのタイマ１９，２０と割り込み論理２１と周辺装置拡張インターフェイス２２とによって与えられる。

【００２８】１７ビット・データバス（ＤＢ）２３が、プロセッサ１０内の複数の機能ブロックの間の通信を与える。プロセッサ１０内の複数のレジスタの大部分は、ＤＢ２３への読取りおよび書込みアクセスを有する。不必要な電力消費を避けるために、また、最大の論理伝播時間を与えるために、複数のバス・ドライバ（不図示）はスタティック・デバイスである。プロセッサ１０の最小命令周期は約１００ｎｓであり、１０ｎ　Ｈｚのプロセッサ・クロック（不図示）が与えられる。

【００２９】図３Ａのデータメモリ１２は、複数の１７ビット並列語として編成されている。語の数は、プロセッサ１０が適用されるアプリケーションにより異なるが、たとえば２５６語から２０４８語の範囲であり、図３には１１５２語が示されている。ＤＭＡＵ１４により与えられる各アドレス５１は、１７ビットのデータがアドレスされるようにする。これらの１７ビットは、実行される命令により異なる多数の方法で作動することができる。大部分の命令について、このデータは１６ビット語フォーマットで解釈される。ＬＡＣＢおよびＳＡＣＢのような２バイト命令は、バイトフォーマットとも呼ばれる８ビット語フォーマットでプロセッサ１０がデータを読み書きするようにさせる。このバイトフォーマット・モードは、アドレスされた１６ビット語の上位バイトまたは下位バイトのどちらかをプロセッサのハードウェアが読み書きするようにさせ、取り出されたバイトはＤＢ２３で右寄せされる。

【００３０】消費者電子製品

このメモリとそれが組み込まれているマイクロプロセッサとは、電話応答機械のような消費者電子製品に使用するように設計されている。本発明を組み込んだ応答機械のブロック図を図４に示す。この装置において、プロセッサ４０２は、電話線インターフェイス４０４とマイクロフォン４０６とスピーカ４０８とに接続されている。マイクロプロセッサ４０２は、電話線インターフェイス４０４経由で電話線４１０上の音響データを送受信する。マイクロプロセッサはまた、スピーカ４０８経由で周辺の領域に音響データを送信し、また、マイクロフォン４０６経由で周辺の領域から音声データを受信できる。

【００３１】代りの実施の形態

一つの代りの実施の形態では、この方式は、セキュリティ回路によりブロックされる命令セットが調節される限りにおいて、符号およびデータの両方を保持するメモリアレー（たとえば、フォンノイマン・アーキテクチャー）内に実装できる。このメモリが組み込まれたマイクロプロセッサは、符号およびデータ・バンクは互いに隔離されているハーバード型アキテクチャーに基づいて設計されているが、本発明はこのアーキテクチャーに全く限定されない。

【００３２】もう一つの代りの実施の形態では、メモリアレイは、二つの保全されたセクションと一つの残りの保全されないままのセクションとに区分される。２つ以上の保全されたセクションが同一データへの読取りアクセスを有することが望ましい場合、または、一つのセクションを開いたままにしておいて、機械にＩＣを設置した後に計算される最終微調整パラメータのセットを記憶させるのが望ましい場合に、これは非常に有用である。

【００３３】好ましい実施の形態に関連して使用することが考えられる他の機能や詳細は、クレームされた発明の実施に必ずしも必要でないが、以下の同時係属出願に開示されている。

【００３４】代理人ドケット番号ＴＩ－２４７０７Ｐ，出願番号６０／０９０，６７０の「可変語長データメモ

リ」。
代理人ドケット番号ＴＩ－２４７０８Ｐ，出願番号６０／０９０，５８９の「チェイン能力つき低コスト乗算器ブロック」。
代理人ドケット番号ＴＩ－２４７１１Ｐ，出願番号６０／０９０，６７１の「高性能マイクロプロセッサで使用するためのフレキシブル・アキュムレータ・レジスタ・ファイル」。
これら全ては、本出願と共に共通に所有され、本発明の出願日と同実の有効な出願日を有し、本書で援用される。

【００３５】修正および変形

当業者に認識されるであろうように、本出願で説明される技術革新的な概念は、非常に広い範囲のアプリケーションにわたり修正され変更し得る。したがって、特許される対称物の範囲は、与えられた特定の例示的な教示のいずれによっても制限されることなく、請求項によってのみ限定される。

【００３６】本出願に開示された好ましい実施の形態は、マイクロプロセッサの内部ＥＰＲＯＭへ組み込まれていて、２つのセクションに分割されたメモリアレイを記述するが、発明の性質の中には、２つだけのセクションに分割したアレイ、内部メモリ、またはメモリのいずれかの特定のタイプにそのアプリケーションを限定するものは何もない。

【００３７】この回路は、このセキュリテイ回路を２重化または多重化して追加のセクション領域を収容できる限りにおいて、３つ以上の保全されたセクションを可能にするように修正できる。これは、エンドユーザがメモリ内にパラメータを記憶させる必要がある場合、または、設置後に最終微調整パラメータをメモリに記憶させる必要がある場合に、有用である。

【００３８】保全メモリはＣＰＵから独立のＩＣ内におくことができる。他の手段を通じてチップの内容に読取りアクセスするのを防止するために、これは若干の追加のセキュリティまたは暗号回路を必要とするであろう。

【００３９】このセキュリティ方式はまた他の形式の非揮発性メモリで実装することもでき、アレイの一部分が読取り専用メモリまたは揮発性メモリでさえあるアレイで実装できる。

【００４０】以上の説明に関して更に以下の項を開示する。

（１）プログラムメモリと、複数のプログラムの少なくとも２つのクラスの間の前記プログラムメモリの部分のためのアクセス特権を指示するセキュリティ・レジスタと、前記プログラムメモリの第１の部分から複数のプログラムの第１のクラスを実行し、前記プログラムメモリの少なくとも１つの他の部分から複数のプログラムの少なくとも１つの他のクラスを実行するために接続されたプログラマブル・プロセッサとを含み、前記プログラムブル・プロセッサ論理は、前記セキュリティ論理の制御の下においてのみ、また、前記セキュリティ論理がデータ・ポインタとアドレス・ポインタとの間の両立可能な所有権を指示するときにのみ、前記メモリにアクセスできる、集積回路。

（２）前記セキュリティ・アクセス制御論理は、前記セキュリティ・レジスタの前記ビットをチェックして、そのビットの少なくともいくつかが補数の状態にあることを保証し、前記セキュリティ・レジスタは１度だけプログラム可能な非揮発性メモリ技術で実装されている、第１項記載の集積回路。

（３）前記集積回路はまた、エミュレーション・モードで作動可能であり、他のあらゆるモードで作動する前に前記エミュレーション・モードを去った後に初期化を起こらせるハードウェア制約を含む、第１項記載の集積回路。

（４）前記セキュリティ・レジスタ内の前記補数のフィールドが、前記ブロックの境界を決定する、第１項記載の集積回路。

【００４１】（５）メモリアレイであって、複数のセクションにグループされた単一のセル・アレイと、前記アレイ内のセルのいずれかに書き込むために接続された書込み回路と、前記アレイ内のセルのいずれかに書き込むために接続された書込み回路と、前記アレイ内のセルのいずれかから読み出すために接続された読出し回路と、前記読出しおよび書込み回路に接続されたメモリ保護回路であって、セクション境界を決定し、前記セクションの１つに記憶されたいずれかの命令により作動することから前記読出しおよび読書き回路を機能抑止し、また、ひとたびメモリ保護回路が使用許可にされれば前記セクションの他に配置されたいずれかのメモリセルを作動することから前記読出しおよび読書き回路を機能抑止する保護レジスタを組み込んでいるメモリ保護回路と、を含む、メモリアレイ。

【００４２】（６）マイクロプロセッサチップであって、再初期化せずにはそのテストモードを変更できない中央処理装置と、該中央処理装置に接続されたプログラムメモリと、プログラムの少なくとも２つのクラスの間で前記プログラムされたメモリの部分へのアクセス特権を指示するセキュリティ・レジスタと、前記メモリに記憶されたデータについて前記メモリの少なくとも第１の部分からプログラムの第１のクラスを実行するとともに第２のクラスを実行するために接続されたプログラマブルプロセッサとを含み、前記セキュリティ論理の制御の下にのみ、また、前記セキュリティ論理がデータ・ポインタとアドレス・ポインタとの間の両立し得る所有権を指示するときにのみ、前記プログラマブルプロセッサ論理が前記メモリにアクセスできる、マイクロプロセッサチップ。

【００４３】（７）電話応答機械であって、再初期化せ

ずにはそのテストモードを変更できない中央処理装置と、該中央処理装置に接続されたプログラムメモリと、プログラムの少なくとも２つのクラスの間で前記プログラムされたメモリの部分へのアクセス特権を指示するセキュリティ・レジスタとを含み、前記セキュリティ論理の制御の下にのみ、また、前記セキュリティ論理がデータ・ポインタとアドレス・ポインタとの間の両立し得る所有権を指示する場合にのみ、前記中央処理装置が前記メモリにアクセスでき、メッセージを受信し送信するような方法で前記中央処理装置を電話線に接続するインターフェイスと、前記応答機械内の記憶のために音響を記録するような方法で前記中央処理装置に接続されたマイクロフォンと、前記応答機械内に記憶された音響をプレイバックするような方法で前記中央処理装置に接続されたスピーカとをさらに含む、電話応答機械。

【００４４】（８）本出願は、ＥＰＲＯＭアレイ２２０内に記憶されたデータおよびプログラム・コードを海賊行為から保護する方法を記述する。非揮発性メモリアレイ２２０は、その設計により２つ以上のブロック２０２に分割される。最初のプログラマーによりプログラムされたコード２０４は、１つ以上のブロック２０２を占め、第１のメモリアドレスから始まる。最初のプログラミングが完了した後に、保護レジスタとして働く最後から２番目のアドレス２０８がセットされて保護ブロック２１０の番号と対応する。これは、セクション境界２１２をセットして、アレイを１次セキュリティ・セクション２１４と２次セキュリティ・セクション２１６とに分割する。１次セキュリティ・セクション２１４の内容は、保護レジスタのビット７（ブロックプロテクト）が使用可能になる（ゼロにセットされる）と、読取り不可で書込み不可にされる。保護レジスタは、保護ブロックの番号およびその反転の両方で書き込まれる。これは、ＥＰＲＯＭが０しか書けないことにより、保護レジスタを不正に変更してセクション境界を移動することを防止する。

【図面の簡単な説明】

【図１】開示されるセキュリティ方式を図示する回路図である。

【図２】セキュリティの理由のために２つのセクションに分割されたメモリアレイを示す図である。

【図３Ａ】混合信号プロセッサのブロック図である。

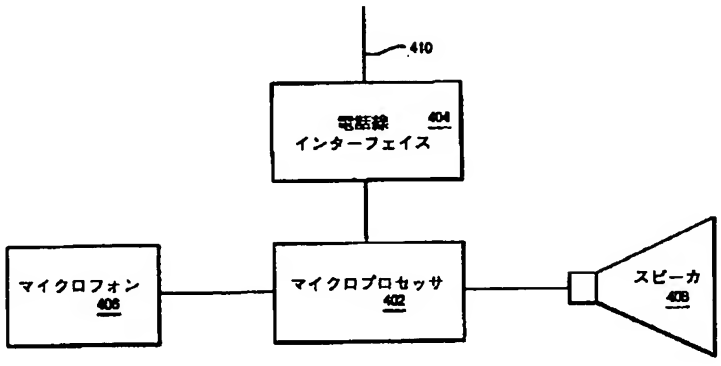
【図３Ｂ】混合信号プロセッサのブロック図である。

【図４】このメモリアレイを使用する電話応答機械を示す図である。

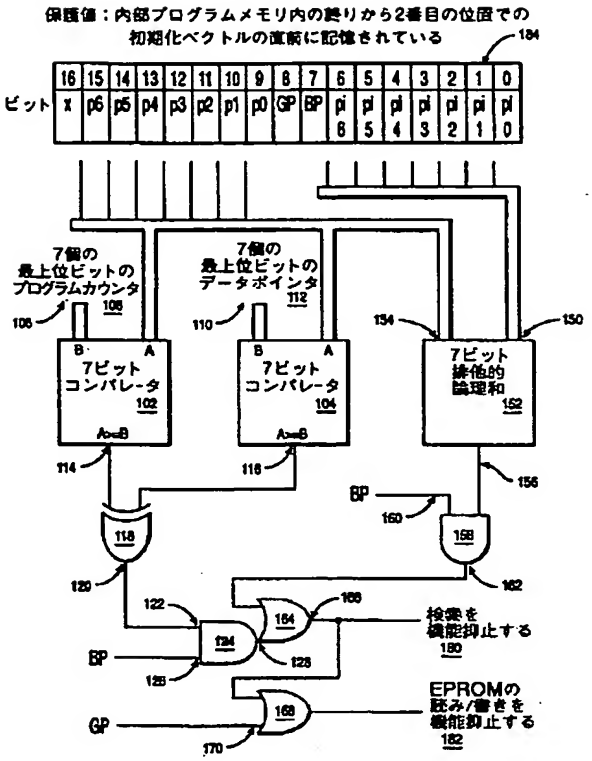
【符号の説明】

２００　アレイ
２０２　ブロック
２０４　コード
２０６　第１のメモリアドレス
２０８　最後から２番目のアドレス
２１０　保護ブロック
２１２　セクション境界
２１４　１次セキュリティ・セクション
２１６　２次セキュリティ・セクション

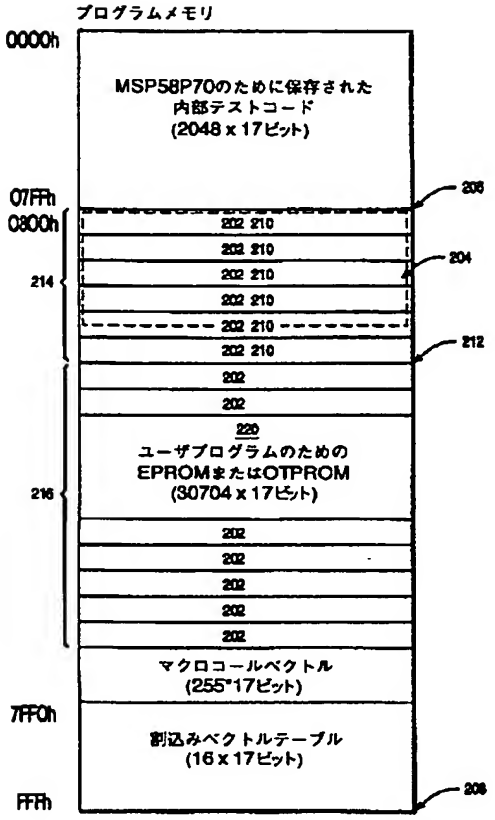
【図４】



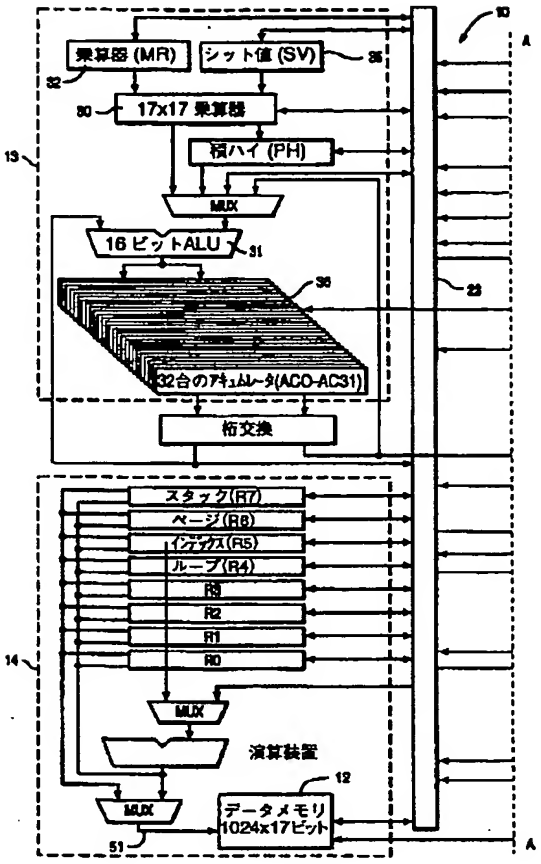
【図１】


保護値：内部プログラムメモリ内の終りから2番目の位置での
初期化ベクトルの直前に記憶されている
184
ビット
16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
x p6 p5 p4 p3 p2 p1 p0 GP BP pi 8 pi 5 pi 4 pi 3 pi 2 pi 1 pi 0
7個の
最上位ビットの
プログラムカウンタ
108
106
7個の
最上位ビットの
データポインタ
112
110
134
150
B A
7ビット
コンパレータ
102
A=B
B A
7ビット
コンパレータ
104
A=B
7ビット
論理和
152
114
116
156
BP
160
118
158
120
162
122
164
166
検索を
機能抑止する
180
BP
124
126
128
EPROMの
読み/書きを
機能抑止する
182
GP
168
170

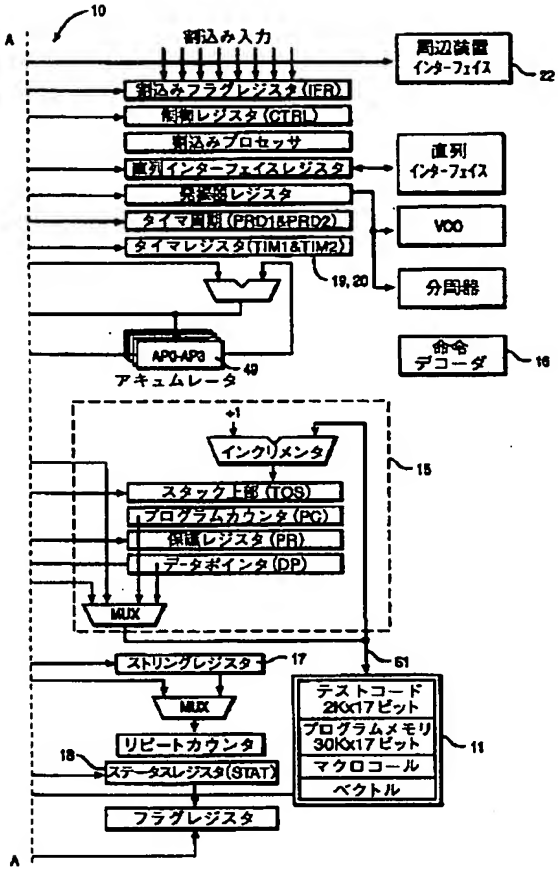
【図２】


プログラムメモリ
0000h
MSP58P70のために保存された
内部テストコード
(2048 x 17ビット)
07FFh
0800h
206
202 210
202 210
202 210
202 210
202 210
204
214
202 210
212
202
202
220
ユーザプログラムのための
EPROMまたはOTPROM
(30704 x 17ビット)
216
202
202
202
202
202
マクロコールベクトル
(255*17ビット)
7FF0h
割込みベクトルテーブル
(16 x 17ビット)
FFFh
208

【図３Ａ】


乗算器 (MR)
シフト値 (SV)
17x17 乗算器
積ハイ (PH)
MUX
16 ビットALU
32台のアキュムレータ(AC0-AC31)
桁交換
スタック(R7)
ページ(R6)
インデクス(R5)
ループ(R4)
R3
R2
R1
R0
演算装置
データメモリ
1024x17ビット

【図３Ｂ】


割込み入力
周辺装置 インターフェイス
割込みフラグレジスタ(IFR)
制御レジスタ(CTRL)
割込みプロセッサ
直列インターフェイスレジスタ
直列 インターフェイス
発振器レジスタ
VCO
タイマ周期(PRD1&PRD2)
タイマレジスタ(TIM1&TIM2)
分周器
AP0-AP3
アキュムレータ
命令 デコーダ
インクリメンタ
スタック上部(TOS)
プログラムカウンタ(PC)
保護レジスタ(PR)
データポインタ(DP)
MUX
ストリングレジスタ
リピートカウンタ
ステータスレジスタ(STAT)
フラグレジスタ
テストコード 2Kx17ビット
プログラムメモリ 30Kx17ビット
マクロコール
ベクトル